IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

UNITED STATES OF AMERICA,	)	Case No. 3:24-CR-00103
	)	
Plaintiff,	)	Judge Thomas M. Rose
	)	
v.	)	
	)	
DAVID SNELL,	)	
	)	
Defendant.	)	

BRIEF IN SUPPORT OF DEFENDANT'S MOTION TO SUPPRESS

Now comes Defendant, David Snell, by and through undersigned counsel, and hereby submits the following brief, in support of his Motion to Suppress, filed herein on February 21, 2025, and seeking to suppress all evidence obtained from Altafiber (subpoenaed as "Fuse Internet Access"); Reddit, Inc.; Alphabet, Inc. (including its subsidiary Google, Inc.); Yahoo! Inc.; and AT&T Corp. (as well as failed to be mentioned or for which Defendant is unaware) as it was obtained without a search warrant and in violation of Defendant's rights under the Fourth Amendment to the United States Constitution, and further moving to suppress all evidence obtained via search warrants issued regarding Defendant David Snell; the property located at 2236 Brookline Avenue, Dayton, Ohio 45420; the 2014 Kia Optima (Lic. Plate No. HBQ4627 and VIN 5XXGN4A70EG272217); as well as all Reddit and Session accounts for which a warrant issued in this matter, as fruit of the poisonous tree.

MEMORANDUM

I. BACKGROUND

On March 26, 2024, the Department of Homeland Security (hereinafter "DHS") issued subpoenas to Fuse Internet Access; Comcast Cable Communications; Charter Communications, LLC; Verizon Wireless; AT&T Corp.; and Reddit, Inc. ECF #33-1-15, PAGEIDs 148-206. Thereafter, in June of 2024, Reddit, Inc. presented private messages between user accounts, including one associated with an email listed in the DHS subpoena. Relying upon these messages, DHS applied for and obtained search warrants for the Defendant's person, his 2014 Kia Optima, his home address, and his user accounts with DropBox, Reddit, and Session on August 27, 2024. ECF #33-16-23, PAGEIDs 207-436.

Defendant was then indicted on November 20, 2024, on charges of Production of Child Pornography in violation of 18 U.S.C. §§2251(a) and (e); Coercion and Enticement in violation of 18 U.S.C. §2422(b); and Receipt of Child Pornography in violation of 18 U.S.C. §§2252(a)(2) and (b)(1). ECF #20, PAGEIDs 72-75.

II. LAW AND ANALYSIS

Evidence in this matter should be suppressed. Evidence was obtained via administrative subpoena and in violation of the warrant requirement of the Fourth Amendment to the United States Constitution; the administrative subpoenas issued in this matter were not sufficiently tailored to the information sought and permitted under the Fourth Amendment; and the search warrants issued relied upon information provided in violation of Defendant's Fourth Amendment rights. As such, all evidence

obtained in this matter, which flows from the administrative subpoenas, is “fruit of the poisonous tree” and should be suppressed.

A. *Evidence Obtained in Response to an Administrative Subpoena Violates the Fourth Amendment’s Warrant Requirement.*

The issuance of administrative subpoenas in this matter is a sidestep of the Fourth Amendment’s warrant requirement as there is no requirement for a showing of probable cause to issue a subpoena.

Under the Fourth Amendment "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause." U.S. Const. amend. IV. “What the Constitution forbids is not all searches and seizures, but unreasonable searches and seizures.” *Elkins v. United States*, 364 U.S. 206, 222, 80 S. Ct. 1437, 1446 (1960). “A ‘search’ occurs when the government infringes upon an expectation of privacy that society is prepared to consider reasonable.’" *United States v. Warshak*, 631 F.3d 266, 284 (6th Cir. 2010)(quoting *United States v. Jacobsen*, 466 U.S. 109, 113, 104 S. Ct. 1652 (1984)). “[T]he ultimate measure of the constitutionality of a governmental search is ‘reasonableness.’ * * * Where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, this Court has said that reasonableness generally requires the obtaining of a judicial warrant” *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 652, 115 S. Ct. 2386, 2390 (1995). This requirement stands to ensure that any inferences supporting a search are “drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime.” *Johnson v. United States*, 333 U.S.

10, 14, 68 S. Ct. 367 (1948). Warrantless searches are *per se* unreasonable, unless conducted pursuant to an exception to the Fourth Amendment's warrant requirement. *United States v. Kennedy*, 427 F.3d 1136, 1140 (8th Cir. 2005).

Moreover, "[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere." *Carpenter v. United States*, 585 U.S. 296, 310, 138 S. Ct. 2206, 2217 (2018). Rather, "what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Katz v. United States*, 389 U.S. 347, 351-352, 88 S. Ct. 507, 511 (1967)(citing *Rios v. United States*, 364 U.S. 253, 80 S. Ct. 1431 (1960); and *Ex parte Jackson*, 96 U.S. 727, 733 (1877)). In fact, the Supreme Court noted in *Carpenter* that it "has never held that the Government may subpoena third parties for records in which the suspect has a reasonable expectation of privacy." *Carpenter*, at 317. The *Carpenter* court warned that "If the choice to proceed by subpoena provided a categorical limitation on Fourth Amendment protection, no type of record would ever be protected by the warrant requirement." *Id.*, at 318. This concern, and *Carpenter's* limitation on administrative powers to obtain records digitally stored with third parties, extends beyond cell-site location information ("CSLI") which was at issue in *Carpenter*.

In *United States v. Warshak*, 631 F.3d 266, 286 (6th Cir. 2010), the Sixth Circuit relied upon what it described as two "bedrock principles." *Id.*, at 288. First, that "the broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards." *Ibid*. Second, the court found axiomatic that "the Fourth Amendment must

keep pace with the inexorable march of technological progress, or its guarantees will wither and perish." *Ibid*. These principles ought to be at the forefront of the Court's determination in the case at bar.

The practice of circumventing Fourth Amendment protections by obtaining a person's private information via administrative subpoena is not a novel practice. As the Government has pointed out in their response to Defendant's Motion to Suppress, this practice has been regular for some time. ECF #33, at PageID 136. Yet, with the above principles in mind, some courts have started questioning the validity of the practice, and rightly so. *Carpenter* represents this trend, finding that a reasonable expectation of privacy exists in cell phone geolocation data, and therefore the Government cannot rely on the third-party doctrine to justify the warrantless search thereof. Similarly, other courts have expressed concern over the expansive use of administrative subpoenas to sidestep the Fourth Amendment's warrant requirements. "The court has concerns about the use of investigatory subpoenas in this case." *United States v. Fritzinger,* 2024 U.S. Dist. LEXIS 120570, *23 (E.D.N.C. 2024).

The Government asserts that the Court in *Fritzinger,* when relaying its concerns regarding the expansive use of administrative subpoenas did so in strict contemplation of future technological advances. ECF #33, at PageID 142-143. This assertion, however, ignores the actual language employed in *Fritzinger*. The court relayed that it was concerned with the present use of administrative subpoenas. It did not, as the Government asserts, merely opine the problems that future technological advancements could afford. That was certainly a concern relayed by the court, and one

worth considering; however, the court also expressed their concern with the present use of administrative or investigative subpoena power to circumvent Fourth Amendment protections.

Here, DHS issued administrative subpoenas in a clear attempt to avoid the probable cause requirements of the Fourth Amendment. In doing so, they violated Defendant's constitutional rights thereunder. Moreover, in addition to the unreasonable nature of using administrative subpoenas to avoid constitutional restraints on Government intrusions, the subpoenas issued in this matter were themselves unreasonably broad, permitting the submission of substantive communications despite the lack of a search warrant for said communications.

B. *The Subpoenas Issued by the Department of Homeland Security were not Sufficiently Limited in Scope, Relevant in Purpose, and/or Specific in Directive*

The DHS subpoenas were not narrowly tailored. *See* ECF #33-1-15, PAGEIDs 148-206. This much is evident both by the language in the subpoenas themselves as well as the fact that the subpoena issued to Reddit resulted in the production of documents outside of the scope of authority of administrative subpoenas. *See* ECF #33-16, 18, 20, and 22, PAGEIDs 241, 244-245, 302, 304-305, 361, 364-365, 418-420, 423-424.

Even if the Court were to ignore the Government's attempted avoidance of the Fourth Amendment's warrant requirement and uphold the use of administrative subpoenas to sidestep the Fourth Amendment, an administrative subpoena will not be considered reasonable unless the request is "[1] sufficiently limited in scope, [2] relevant in purpose, and [3] specific in directive so that compliance will not be unreasonably

burdensome." *Carpenter*, 585 U.S. at 330. A subpoena which is not sufficiently limited in scope, relevant in purpose, and which is unreasonably burdensome is therefore an unreasonable search under the Fourth Amendment. *Ibid*.

Here, the DHS subpoenas to Fuse, Comcast, Charter, and Verizon, made vague requests regarding subscriber communications and records;

> **Subscriber Information:** For the IP address(es) listed below, any and all subscriber and customer information, including but not limited to: (1) subscriber name; (2) physical, billing and email address; (3) service or subscriber agreements; (4) length of service (including start date); (5) identification of account number; (6) means and source of payment for service (including any credit card or bank account number); ***(7) account logs or other logs reflecting account usage;*** (8) types of service; (9) additional screen names (including instant message) and Internet Protocol (IP) logs.

ECF #33-1, 4, 9, 13, and 15, at PageIDs 150, 162, 182, 190, 198, and 205. (emphasis added).

The subpoenas' vague language was tantamount to a *de facto* request for content since it contained overbroad requests for "account logs or other logs reflecting account usage." *Ibid*. No clarification is provided in the subpoena which would exclude the disclosure or provision of the contents of communications and the plain language of the subpoena could easily be interpreted to include substantive communications. Similarly, in their subpoena to AT&T, DHS requested extensive records, including requests for the content of communications between alleged subscribers and third parties:

> **Subscriber Information:** The names; addresses; length of services including start date, close date if the account is closed, types of services utilized (e.g. push-to talk, text, three-way calling, data, etc.); means and sources of payment (including any and all credit cards and bank account numbers) of a subscriber to and customer of such service; and all

> telephone instrument numbers and other subscriber numbers of identity, including temporarily assigned network address for all subscribed communication services.
>
> **Call Information**: ***Local and long-distance connection records (including all incoming and outgoing calls; and all voice, VoLTE, SMS, MMS, text, and data usage)*** and all records of session times and durations; and all telephone instrument numbers and other subscriber numbers or identity, including temporarily assigned network address for all subscribed communication services.

ECF #33-7 and 12, at PageIDs 172 and 194. (emphasis added).

Once again, the subpoenas language, requesting records of all incoming and outgoing calls, voice, VoLTE, SMS, MMS, text, and data usage lends itself to broad interpretation. *Ibid*. Again, no clarification is provided in the subpoena which would exclude the disclosure or provision of the contents of communications and the plain language of the subpoena could easily be interpreted to include substantive communications. Finally, in their subpoenas to Reddit, DHS included a catchall which permitted broad interpretation of the scope of requested data.

> **Child Exploitation**: ***This subpoena is in regard to an investigation involving Child Exploitation and/or transmission of Child Pornography via the internet. Please do not disclose/notify the user of the issuance of this subpoena. Disclosure to the user could impede an investigation or obstruct justice.***
>
> Please provide basic subscriber information for any Reddit accounts (including deleted accounts) associated with the following email addresses (whether verified or not) during the following date range. ***This information should include, but not be limited to:***
>
> Username/subscriber identity, IP logs with port numbers (including registration IP), account creation date/time, and the user's name, email address, and phone number…
>
> *****This investigation involves child safety. Please do not notify the users associated with the below accounts.*****

ECF #33-14, PageID 202. (emphasis added).

Specifically, DHS subpoenaed Reddit three (3) times, requesting information regarding various user accounts and unknown accounts associated with various email addresses. ECF #33-3, 14, PAGEIDs 158 and 202. The catch-all contained within the subpoenas issued to Reddit allowed for expansive interpretation regarding what specifically was being requested. *Ibid*. Given the disclosure that the Government was seeking information pursuant to an investigation into the transmission of child pornography, along with the overly broad catch-all, an expansive interpretation of the requested information was almost a certainty. This defect in the subpoena to Reddit is even more clear in light of the fact that after receiving the subpoena from DHS, Reddit produced the content of private messages between a user account associated with the IP address requested (which had previously been provided by Reddit) and another Reddit user. ECF #33-16, 18, 20, and 22, PAGEIDs 241, 244-245, 302, 304-305, 361, 364-365, 418-420, 423-424.

The issue then turns upon whether an individual's expectation of privacy in the things sought is objectively reasonable. *Jacobsen*, 466 U.S. at 104. It has long been established that a person has a reasonable expectation of privacy in their private communications with others. *Jacobsen*, 466 U.S. at 114; *Ex Parte Jackson*, 96 U.S. at 733. A reasonable expectation of privacy exists in an individual's email. *In Re Grand Jury Subpoena v. Kitzhaber*, 828 F.3d 1083, 1090 (9th Cir. 2016). Specifically, the court in *Kitzhaber* determined that email communications should be viewed similarly to mail, in whose contents a person has a reasonable expectation of privacy. *Ibid* (citing to

United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2008)). This reasonable expectation of privacy exists in phone calls, even phone calls made in public. *Katz*, 389 U.S. at 352. "[T]rusting a letter to an intermediary does not necessarily defeat a reasonable expectation that the letter will remain private". *Id.*, at 351. It logically flows that direct messaging, private messaging, and other non-public communications between parties would enjoy this same expectation of privacy. *See Warshak, supra*. "Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection." *Id.*, at 285-286.

> [I]t is manifest that agents of the government cannot compel a commercial ISP to turn over the contents of an email without triggering the Fourth Amendment. An ISP is the intermediary that makes email communication possible. Emails must pass through an ISP's servers to reach their intended recipient. Thus, the ISP is the functional equivalent of a post office or a telephone company. As we have discussed above, the police may not storm the post office and intercept a letter, and they are likewise forbidden from using the phone system to make a clandestine recording of a telephone call—unless they get a warrant, that is.

Warshak, 631 F.3d at 286.

This reasonable expectation of privacy is not diminished by the presence or right of a third-party intermediary. The *Warshak* court relied, in part, on the established doctrine of rented space, wherein tenants and hotel guests maintain a reasonable expectation of privacy despite the potential and periodic intrusion occasioned by access granted to landlords, housekeepers, handymen, and other third parties. *See United States v. Allen*, 106 F.3d 695, 699 (6th Cir. 1997); *United States v. Washington*, 573 F.3d 279, 284 (6th Cir. 2009).

> [T]he mere ability of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy. * * * Therefore, the threat or possibility of access is not decisive when it comes to the reasonableness of an expectation of privacy. Nor is the right of access[;] * * * at the time Katz was decided, telephone companies had a right to monitor calls in certain situations. Specifically, telephone companies could listen in when reasonably necessary to "protect themselves and their properties against the improper and illegal use of their facilities." [Citation omitted]. * * * Thus, under *Katz*, the degree of access granted to [a third-party intermediary] does not diminish the reasonableness of Warshak's trust in the privacy of his emails.

Warshak, 631 F.3d at 286-287.

Here, as it regards the private messages involving user accounts alleged to belong to Defendant, Reddit is a third-party intermediary. The communications provided after receipt of the defective subpoena were sent *via* Reddit rather than *to* Reddit and are thus analogous to those communications at issue in *Warshak, Jacobsen, Jackson, Kitzhaber, and Forrester*. Therefore, the third-party doctrine cannot legitimize the disclosure of said communications nor the overly broad subpoena which issued prior thereto. Even setting aside the overbreadth of the subpoenas and the resulting unlawful disclosure, DHS violated Defendants' Fourth Amendment rights by even viewing and then, as discussed below, using the private messages provided by Reddit after their receipt of the subpoena to obtain search warrants. ECF #33-16, 18, 20, and 22, PAGEIDs 241, 244-245, 302, 304-305, 361, 364-365, 418-420, 423-424.

As such, the administrative subpoenas issued by DHS in this matter are materially defective and are tantamount to unreasonable searches under the Fourth Amendment. Because of this, any evidence received in response to, or flowing from, the DHS subpoenas ought to be suppressed.

C. *The Search Warrants Issued Relied Upon Information Obtained Absent a Warrant and After Issuance of Overbroad Administrative Subpoenas*

The Government requested, and was granted, search warrants regarding the Defendant's person, vehicle, home, and online accounts based upon information unlawfully obtained in response to administrative subpoenas. *See* ECF #33-16, 18, 20, and 22, PAGEIDs 241, 244-245, 302, 304-305, 361, 364-365, 418-420, 423-424. The probable cause determination supporting the issuance of these search warrants was rooted in the information illegally obtained by DHS. *See* ECF #33-17, 19, 21, and 23, PAGEIDs 260, 320, 380, and 431.

Under the Fourth Amendment, no warrants shall issue but upon probable cause, supported by oath or affirmation. U.S. Const. amend IV. "It is now fundamental that evidence which is obtained as a direct result of an illegal search and seizure may not be used to establish probable cause for a subsequent search." *United States v. Wanless*, 882 F.2d 1459, 1465 (9th Cir. 1989)(citing to *United States v. Vasey*, 834 F.2d 782, 788 (9th Cir. 1987); *United States v. Roberts*, 747 F.2d 537, 541 (9th Cir. 1984); and *Wong Sun v. United States*, 371 U.S. 471, 487-88, 83 S. Ct. 407 (1963)). It is thus elementary that "[e]vidence discovered pursuant to a warrant will be inadmissible if the warrant was secured from a judicial officer through the use of illegally acquired information." *United States v. Oakley*, 944 F.2d 384, 386 (7th Cir. 1991)(citing *Silverthorne Lumber Co. v. United States*, 251 U.S. 385, 391-392 (1920)).

Here, search warrants issued a on August 27, 2024, regarding Defendant's person, the property located at 2236 Brookline Avenue, Dayton, Ohio 45420, the Kia Optima bearing Lic. Plate No. HBQ4627 and VIN 5XXGN4A70EG272217, as well as

several Reddit, Session, and Dropbox accounts. *See* ECF #33-17, 19, 21, and 23, PAGEIDs 260, 320, 380, and 431. Each warrant relies upon information received in response to the administrative subpoenas issued to Fuse, ODJFS, Google, Comcast, Charter, Verizon, AT&T, and Reddit. *See* ECF #33-16, 18, 20, and 22, PAGEIDs 241, 244-245, 302, 304-305, 361, 364-365, 418-420, 423-424. As established herein the administrative subpoenas violated Defendant's Fourth Amendment rights by nature of their use in circumventing the warrant requirement as well as their vagueness and overbreadth. Most damning, information from Reddit including the content of communications, specifically private messages, between Reddit users, received after Reddit was served with a subpoena for user information on March 26, 2024, was instrumental in the probable cause determination which supported the warrants. *See* ECF #33-16, 18, 20, and 22, PAGEIDs 241, 244-245, 302, 304-305, 361, 364-365, 418-420, 423-424; *c.f.* ECF #33-17, 19, 21, and 23, PAGEIDs 260, 320, 380, and 431.

As such, the warrants issued in this matter rely upon improperly obtained evidence and therefore do not satisfy the warrant requirement of the Fourth Amendment. Any evidence obtained pursuant to the warrants issued herein should therefore be suppressed.

III. CONCLUSION

The Government's use of administrative subpoenas in place of a valid and necessary search warrant violated Defendant's rights under the Fourth Amendment of the United States Constitution.

Even if the use of administrative subpoenas were valid in this matter, a point which Defendant does not concede, the subpoenas at issue were unreasonably overbroad. Specifically, the subpoenas were written in such a manner that substantive communications fit within the confines of responsive information and/or documents. This resulted in the provision of substantive communications between user accounts alleged to belong to Defendant and other Reddit users. Such communications do not fall within the third-party doctrine. The subpoenas, therefore, requested documents which, even adopting the Government's point of view, are outside the boundaries permitted by the Fourth Amendment. Thus, even in viewing the Fourth Amendment's relationship with the administrative subpoenas at issue from the Government's perspective, the information received from Reddit required a search warrant. This was not timely obtained. Rather, this unlawfully obtained information was then used in support of the warrant application. Absent these warrantless searches, and unreasonable subpoenas, information contained within the affidavits could not come anywhere close to setting forth the probable cause necessary to comply with the Fourth Amendment.

As the search warrants issued in this case relied upon information unlawfully obtained, by overbroad, and unlawful administrative subpoenas, any evidence obtained through their execution is fruit of the poisonous tree and must be suppressed. Similarly, all evidence flowing from the administrative subpoenas themselves must also be suppressed.

Wherefore, Defendant submits that this Court should suppress all evidence flowing from the Administrative Subpoenas issued by Homeland Security.

Respectfully submitted,

/s/Anthony R. Cicero
Anthony R. Cicero (0065408)
Timothy R. Saunders (0098595)
CiceroAdams, LLC
500 East Fifth Street
Dayton, Ohio 45402
(937) 424-5390
(937) 424-5393 (Fax)
tonycicero@gocicero.com
timsaunders@gocicero.com
ATTORNEYS FOR DEFENDANT

CERTIFICATE OF SERVICE

I hereby certify that on May 7, 2025, the foregoing was electronically filed with Clerk of Court using the CM/ECF system which will send notification of such filing to Christina E. Mahy, Assistant United States Attorney, 602 Federal Building, 200 West Second Street, Dayton, Ohio 45402.

/s/Anthony R. Cicero
ANTHONY R. CICERO (0065408)